LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-JRNL-651543

Indicator Sharing Made Easy with MBL

M. M. Myrick

March 10, 2014

Indicator Sharing Made Easy with MBL

Disclaimer

Indicator Sharing Made Easy With MBL

The Master Block List (MBL) is a malware indicator aggregation service sponsored by the Lawrence Livermore National Laboratory (LLNL) with funding from the Department of Energy (DOE). MBL was originally developed in 2008 by cyber security analysts at several national DOE laboratories. In search of a simple way to automatically share information related to cyber attacks, they quickly became frustrated with the lack of available options and decided to create their own framework. Over six years later, MBL remains a simple, easy to use repository, optimized for automatic submission and retrieval of cyber attack information.

As technology and cyber security continue to evolve, so does the MBL framework. Recently, the backend for MBL was migrated to Splunk® and leverages a purpose-built Splunk application called Parthenon. Even though Splunk is not free, its simplicity and ease of use could not be beat, so LLNL decided to pay for the license so that cyber defenders throughout DOE and strategic commercial partners could benefit from MBL as well.

Through the use of MBL, participants are able to leverage the intelligence of the collective to more effectively defend against cyber attacks. If you would like to learn more about MBL and how you can participate, please contact Matthew Myrick at LLNL (myrick3@llnl.gov).

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.